(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－189721
（P2001－189721A）
(43)公開日　平成13年７月10日(2001.7.10)

(51)Int.Cl.'	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１Ｂ
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ	7/26	１０９Ｒ
Ｈ０４Ｌ　9/12		Ｈ０４Ｌ	9/00	６０１Ｅ
				６３１

審査請求　未請求　請求項の数８　ＯＬ　（全 19 頁）

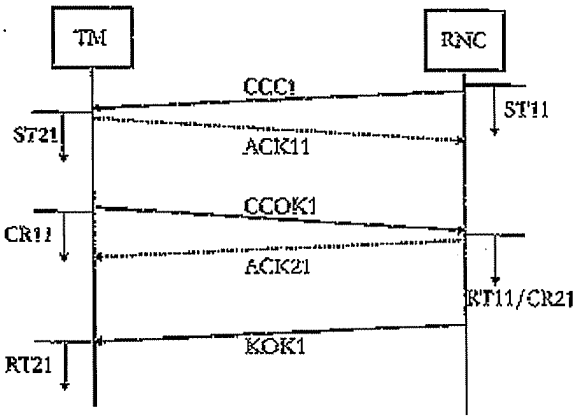
(21)出願番号　特願2000－363624(P2000－363624)
(22)出願日　平成12年11月29日(2000.11.29)
(31)優先権主張番号　１９９５７３８７．５
(32)優先日　平成11年11月29日(1999.11.29)
(33)優先権主張国　ドイツ（ＤＥ）
(31)優先権主張番号　１９９５８００４．９
(32)優先日　平成11年12月２日(1999.12.2)
(33)優先権主張国　ドイツ（ＤＥ）
(31)優先権主張番号　１００２１８３．２
(32)優先日　平成12年１月19日(2000.1.19)
(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　5621　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(72)発明者　クリストフ　ヘルマン
ドイツ連邦共和国，52064　アーヘン，カゼルネンシュトラーセ　6
(74)代理人　100070150
弁理士　伊東　忠彦　（外１名）

最終頁に続く

(54)【発明の名称】　暗号鍵交換手順を有する無線ネットワーク

(57)【要約】
【課題】　本発明の目的は，異なる暗号変更手順を有する無線ネットワークを提供することである。
【解決手段】　本発明は，トラフィック及び，制御チャネルを介して伝送されるべき特定のデータを符号化しかつ特定の時に符号化のために必要な暗号鍵をそれぞれ変更するために設けられた，無線ネットワーク制御装置と複数の割り当てられた端末を含む無線ネットワークに関する。無線ネットワーク制御装置は，古い暗号鍵で符号化された暗号鍵変更に関するメッセージを端末へ伝送する。端末は，新たな暗号鍵の受取通知として，新たな暗号鍵で符号化されたメッセージで無線ネットワーク制御装置へ応答する。



1

【特許請求の範囲】

【請求項１】　伝送されるべき特定のデータを符号化しかつ特定の時に符号化のために必要な暗号鍵をそれぞれ特定のときに変更するために設けられた、無線ネットワーク制御装置と複数の割り当てられた端末を含む無線ネットワークであって、

無線ネットワーク制御装置は、古い暗号鍵で符号化された暗号鍵変更に関するメッセージを端末へ伝送するために設けられ、且つ、

端末は、新たな暗号鍵の受取通知として、新たな暗号鍵で符号化されたメッセージを無線ネットワーク制御装置へ伝送するために設けられたことを特徴とする無線ネットワーク。

【請求項２】　無線ネットワーク制御装置は、古い暗号鍵で符号化された暗号変更命令を端末に送信するようになされ、かつ、

端末は、新たな暗号鍵で符号化された暗号変更命令を無線ネットワーク制御装置に送信するようになされることを特徴とする請求項１記載の無線ネットワーク。

【請求項３】　無線ネットワーク制御装置により送信される暗号変更命令は、新たな暗号鍵を含むことを特徴とする請求項１記載の無線ネットワーク。

【請求項４】　無線ネットワーク制御装置は、受信した鍵が送信した鍵と一致するときには、一致命令を端末へ送信するようになされたことを特徴とする請求項３記載の無線ネットワーク。

【請求項５】　端末が一致命令又は新たな暗号鍵で符号化されたデータを受信したときには、端末は、データの符号化のために無線ネットワーク制御装置から受信した鍵を使用するために設けられていることを特徴とする請求項４記載の無線ネットワーク。

【請求項６】　無線ネットワーク制御装置は、暗号変更の開始時に、データユニットの伝送の停止が成されることを特徴とする請求項１記載の無線ネットワーク。

【請求項７】　新たな暗号鍵の有効性の瞬間に関するメッセージが交換された後、無線ネットワーク制御装置は、少なくとも１つの端末が新たな暗号鍵を使用しているか否かをも確認し、確認後に、新たな暗号鍵又は古い暗号鍵での確認結果に基づき、データユニットの伝送を開始することを特徴とする請求項６記載の無線ネットワーク。

【請求項８】　無線ネットワーク制御装置と少なくとも１つの端末は、データユニット番号を蓄積し且つ同期フェーズ中にデータユニットで使用される鍵を特徴とし、同期フェーズは、無線ネットワーク制御装置又は端末のいずれかからの新たな暗号鍵で符号化された最初のデータユニットの送信と共に開始し、且つ、無線ネットワーク制御装置又は端末のいずれかからの古い暗号鍵で符号化された最後のデータユニットの繰返された送信と共に終了することを特徴とする請求項１記載の無線ネットワーク。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、伝送されるべき特定のデータを符号化しかつ特定の時に符号化のために必要な暗号鍵をそれぞれ変更するために設けられた、無線ネットワーク制御装置と複数の割り当てられた端末を含む無線ネットワークに関する。

【０００２】

【従来の技術】１９９２年のＶｅｒｌａｇＣｅｌｌ＆Ｓｙｓ．Ｍｉｃｈｅｌ　Ｍｏｕｌｙ及び．Ｍａｒｉｅ－Ｂｅｒｎａｄｅｔｔｅ　Ｐａｕｔｅｔによる"移動通信のためのＧＭＳシステム"３９１頁から３９５頁より、データは無線ネットワーク制御装置と端末間で符号化された形式で伝送されることが知られている。伝送に必要な暗号鍵は、特定の時間間隔で変更される。このために３つのステップが設けられる。

【０００３】

【発明が解決しようとする課題】本発明の目的は、異なる暗号変更手順を有する無線ネットワークを提供することである。

【０００４】

【課題を解決するための手段】この目的は、前文で述べた形式の、無線ネットワーク制御装置は、古い暗号鍵で符号化された暗号鍵変更に関するメッセージを伝送するために設けられ、且つ、端末は、新たな暗号鍵の受取通知として、新たな暗号鍵で符号化されたメッセージを無線ネットワーク制御装置へ伝送するために設けられた無線ネットワークにより達成される。

【０００５】本発明に従った無線ネットワークは、複数の無線セルを有し、その中のそれぞれの無線ネットワーク制御装置と複数の端末は、無線で、制御データとペイロードデータを送信する。無線伝送は、例えば、無線、ウルトラシェル又は、赤外経路を介して、情報信号を伝送するために設けられる。

【０００６】本発明に従って、端末は新たな暗号鍵で符号化されたメッセージを通知し、そのメッセージは、新たな暗号鍵で符号化されたメッセージ（例えば、暗号鍵命令の受取通知）を送信することによる暗号鍵の変更（例えば、暗号変更命令）に関する。端末が新たな暗号鍵を間違って通知されたときには、暗号鍵を受取通知する命令は検出されない。従って、新たな暗号鍵は使用できない。

【０００７】

【発明の実施の形態】図１は、例えば、無線ネットワーク制御装置（ＲＮＣ）１と複数の端末２から９を有するラジオネットワークのような無線ネットワークを示す。無線ネットワーク制御装置１は、例えば、端末２から９のような無線トラフィックに関化している全構成要素を制御する。制御とペイロードデータの変更は少なくとも

無線ネットワーク制御装置１と端末２から９の間で発生する。無線ネットワーク制御装置１は、ペーロードデータを伝送するためのそれぞれのリンクを確立する。

【０００８】通例として、端末２から９は、移動装置であり、無線ネットワーク制御装置１は、固定されている。無線ネットワーク制御装置１は、移動可能でも良い。

【０００９】無線ネットワークでは、例えば、ＦＤＭＡ（周波数分割多重アクセス），ＴＤＭＡ（時分割多重アクセス）又は、ＣＤＭＡ（符号分割多重アクセス）法に従った無線信号、又は、それらの方法の結合に従った無線信号が伝送される。

【００１０】特別な符号拡散法であるＣＤＭＡ法によれば、ユーザからのバイナリ情報（データ信号）は、異なる符号シーケンスで多回変調される。そのような符号シーケンスは、擬似ランダム矩形波信号（擬似ノイズコード）を有し、そのレートは、チップレートと呼ばれる。擬似ランダム矩形波信号の矩形はパルスの継続時間は、チップ間隔Ｔｃと呼ばれる。１／Ｔｃはチップレートである。擬似ランダム矩形は信号とデータ信号の乗算又は、変調はそれぞれ、拡散計数Ｎｃ＝Ｔ／Ｔｃのスペクトラム拡散となる。ここで、Ｔはデータ信号の矩形はパルスの継続時間である。

【００１１】ペイロードデータと制御データは、少なくとも１つの端末（２から９）と無線ネットワーク制御装置１の間で、無線ネットワーク制御装置１により予め定められたチャネルを介して伝送される。チャネルは、周波数範囲、時間範囲及び、ＣＤＭＡ方では拡散コードにより決定される。無線ネットワーク制御装置１から端末２から９への無線リンクはダウンリンクと呼ばれ、端末から無線ネットワーク制御装置へのリンクはアップリンクと呼ばれる。このように、データは、無線ネットワーク制御装置から端末へダウンリンクを介して伝送され、また、端末から無線ネットワーク制御装置へはアップリンクを介して伝送される。

【００１２】ダウンリンクチャネルが設けられ、接続設定に先立ち、無線ネットワーク制御装置１から端末２から９へ制御データを放送するのに使用される。そのようなチャネルは、ダウンリンク放送制御チャネルと呼ばれる。接続設定に先立ち、端末２から９から無線ネットワーク制御装置１へ制御データを送信するために、無線ネットワーク制御装置１に割り当てられているアップリンク制御チャネル使用できるが、しかし、それは、他の端末２から９によってもアクセスされる。種々の又は全ての端末２から９により使用されるアップリンクチャネルは、共通アップリンクチャネルと呼ばれる。例えば、端末２から９と無線ネットワーク制御装置１の間の接続の設定後に、ペイロードデータは、ダウンリンク又は、アップリンクユーザチャネルを介して伝送される。ただ１つの送信器と１つの受信器間で設定されるチャネルは専用チャネルと呼ばれる。通例として、ユーザチャネルは、リンクに特定の制御データを伝送するための専用の制御チャネルに関連する専用のチャネルである。

【００１３】端末２から９を無線ネットワーク制御装置１内に有するために、信号化されたＲＡＣＨチャネル（ランダムアクセスチャネル）と呼ばれる、競合チャネルは十分である。データパケットは、そのような信号化されたＲＡＣＨチャネル上で伝送され得る。

【００１４】ペイロードデータを無線ネットワーク制御装置１と端末間で交換することができるためには、端末２から９は、無線ネットワーク制御装置１と同期していることが必要である。例えば、ＦＤＭＡとＴＤＭＡ法の結合が使用されるＧＳＭシステム（移動通信のためのグローバルシステム）から、好適な周波数範囲の決定の後に、データ伝送のシーケンス化内でフレー同期を助ける。所定のパラメータに基づいて、フレームの時間依存に値が決定（フレーム同期）されることが知られる。そのようなフレームは、ＴＤＭＡ，ＦＤＭＡ及び、ＣＤＭＡ法の場合には、常に、端末と無線ネットワーク制御装置のデータの同期には必要である。そのようなフレームは種々のサブフレームを含み又はいくつかの他の連続するフレームと共にスーパーフレームを形成する。簡単のために、基準フレームとして参照されるフレームは開始されたフレームからである。

【００１５】無線ネットワーク制御装置１と端末２から９の間の無線インターフェースを介した制御データの交換を、図２に示すレイヤモデル又は、プロトコル構造を参照して説明する（例えば、第３世代パートナッシッププロジェクト（３ＧＰＰ）；技術仕様グループ（ＴＳＧ）ＲＡＮ；ワーキンググループ２（ＷＧ２）；無線インターフェースプロトコル構造；ＴＳ２５．３０１Ｖ３．２（１９９０－１０））。レイヤモデルは、３つのプロトコルレイヤを有する。物理レイヤＰＨＹ、サブレイヤＭＡＣとＲＬＣ（図２では種々の形式のサブレイヤＲＬＣを含む）データリンクレイヤと、レイヤＲＲＣである。サブレイヤＭＡＣは、媒体アクセス制御のためであり、サブレイヤＲＬＣは、無線リンク制御のためであり、レイヤＲＲＣは無線資源制御のためである。．レイヤＲＲＣは端末２から９と無線ネットワーク制御装置１間の通信に責任がある。サブレイヤＲＬＣは、端末２から９と無線ネットワーク制御装置１間の無線リンクを制御するのに使用される。レイヤＲＲＣは、サブレイヤＭＡＣとＰＨＹを制御リンク１０と１１を介して制御する。このように、レイヤＲＲＣはサブレイヤＭＡＣとＰＨＹのコンフィグレーションを制御できる。物理レイヤＰＨＹは、サブレイヤＭＡＣへの搬送リンクを提供する。サブレイヤＭＡＣは、サブレイヤＲＬＣへ有効な論理接続１３を行う。サブレイヤＲＬＣはアクセス点１４を介して、アプリケーションにより到達できる。

【００１６】そのような無線ネットワークでは、認証さ

れていない方法により盗聴されることを避けるために安全性と信頼性のために、データは符号化された形式で無線インターフェースを介して伝送される。符号化はデータ接続レイヤ（例えば、レイヤＲＬＣ又は、ＭＡＣ内の）データ接続レイヤで行われる。図３に示すように、データＤは符号化マスクＭと、排他的論理語機能（ＸＯＲ）を介して結合され、それにより、符号化データストリームＣ＿Ｄを得る。符号化マスクＭは、符号化アルゴリズムに従って動作する符号化機能１６内で形成され、そして、入力値として、暗号鍵ＣＫとここでは示していない他のパラメータＰを受信する。

【００１７】暗号鍵は、無線ネットワーク制御装置１と端末２から９の両方で知られていなければならない。暗号鍵は特定の時点で（例えば、１時間おきに）暗号鍵変更と呼ぶ特別の手順で変更される。

【００１８】以下は、５つの異なる暗号鍵変更ＣＫＣ１からＣＫＣ５を示す。図４を参照して、第１の手続ＣＫＣ１を説明する。第１の手順ＣＫＣ１では、新たな暗号鍵が特に他の４つの手続ＣＫＣ２からＣＫＣ５へ共に送信される。最初に無線ネットワーク制御装置１（図１ではＲＮＣと参照される）は、各端末へのデータの送信（ダウンリンク）を停止する。そのデータは、符号化される（ＳＴ１１）。１つの例外は暗号鍵変更命令ＣＣＣ１であり以後説明する。受信されたアップリンクデータは、更に有効な暗号鍵でマスクが解除される。そして、無線ネットワーク制御装置１（ＲＮＣ）は、端末（図４で、ＴＭとして参照）へ、新たな暗号鍵と共に暗号鍵変更命令ＣＣＣ１を信号チャネルを介して送る（古い暗号鍵で符号化されている）。安全に関し、変更ＣＫＣに先立ち伝送され且つ古い暗号鍵で符号化されるがしかし通知されずに（通知なしのままで）、変更ＣＫＣ１後に新たにされた伝送があるときに新たな暗号鍵でデータが符号化されるか否かは重要でない。

【００１９】端末が新たな暗号鍵と共に暗号鍵変更命令ＣＣＣ１を受信後、１つの受取通知命令ＡＣＫ１１のみが無線ネットワーク制御装置１に転送され、それにより、所定の時間期間経過後、無線ネットワーク制御装置１は新たな暗号鍵と共に暗号鍵変更命令ＣＣＣ１を再び送信しない。符号化されるべき各データの転送（アップリンク）も、端末（ＳＴ２１）により停止される。唯一の例外は以下に説明するような古い暗号鍵で符号化された暗号鍵受取通知命令ＣＣＯＫ１である。それぞれの端末が暗号鍵を暗号鍵変更命令ＣＣＣ１から取り出し後、端末により暗号鍵変更命令ＣＣＣ１から取り出された鍵は新たな暗号鍵として登録されそして、暗号鍵受取通知命令ＣＣＯＫ１と共に無線ネットワーク制御装置１へ送信される。暗号鍵受取通知命令ＣＣＯＫ１の送信後、端末はデータを受信し且つ古い暗号鍵と新しい暗号鍵でデータを暗号化する位置にある。古い暗号鍵は、古い暗号鍵で符号化された更新する暗号鍵変更命令ＣＣＣ１が受信されたときのみ必要である。これは、例えば、伝送エラーの結果のような暗号鍵受取通知命令ＣＣＯＫ１内に含まれる暗号鍵が元の伝送された暗号鍵と異なるときに起こる。

【００２０】暗号鍵受取通知命令ＣＣＯＫ１受信は無線ネットワーク制御装置１により受取通知命令ＡＣＫ２１により端末に通知され、端末へのデータ伝送（ダウンリンク）は新たな暗号鍵と共に回復される。回復は元の伝送された鍵（ＳＴ１１）が暗号鍵受取通知命令ＣＣＯＫ１内に含まれる鍵と一致するときにのみ発生する。受信されたデータは、新たな暗号鍵（ＣＲ２１）でマスクが解除される。そして、無線ネットワーク制御装置１は、一致命令ＫＯＫ１を端末に送る。前述のように、暗号鍵変更命令ＣＣＣ１の送信は暗号鍵が一致しないときは繰り返される。この一致命令ＫＯＫ１又は、新たな暗号鍵で符号化されたデータ（ダウンリンク）を受信後、端末は新たな暗号鍵（ＲＴ２１）でデータ伝送（アップリンク）を開始する。これは、手順ＣＫＣ１を終了指す且つデータ伝送はこの暗号かぎのみで効果がある。

【００２１】端末は旧及び新暗号鍵の両方でＣＲ１１とＲＴ２１間で受信されたデータを解読するということの結果、端末は、手順ＣＫＣ１が成功的に終了された（そして端末は古い暗号鍵で符号化された一致命令ＫＯＫ１を受信する）か、又は、手順は新たに開始されるべきか（この場合には端末は例えば、新たな暗号鍵を再び含む暗号鍵変更命令ＣＣＣ１を受信する）を認識する。これは、間違って受信された鍵の結果として、端末とネットワーク間の全ての接続が壊されるのを避ける。

【００２２】第１の例の上述の手順ＣＫＣ１は、信号リンクにのみ関連する。データ伝送の繰返しと共に働くデータリンクは、それぞれのレイヤＲＬＣも停止命令（端末：ＳＴ２１、ネットワークＳＴ１１）、又は、ペイロードデータの伝送を回復する命令（端末ＲＴ２１、ネットワークＳＴ２１）が通知される手順中に含まれる。

【００２３】第２の暗号鍵変更ＣＫＣ２を図５を参照して以下に説明する。この変更ＣＫＣ２と共に、端末（ＴＭ）は別のデータ変更手順（図示していない）内で新たな暗号鍵に関する情報を受信する。暗号鍵自身が無線インターフェースで伝送されることが避けられる。この変更ＣＫＣ２で、古い暗号鍵から新たな暗号鍵への同期した変更が端末と無線ネットワーク制御装置１（ＲＮＳ）間で行われる。最初に、符号化されたデータの端末への各伝送（ダウンリンク）は、無線ネットワーク制御装置１（ＳＴ２１）により停止される。唯一の例外は、以下に説明する暗号鍵変更命令ＣＣＣ２である。受信されたアップリンクデータは、これまでに使用された暗号鍵でさらに符号化される。そして、（古い暗号鍵で符号化された）暗号鍵変更命令ＣＣＣ２は、無線ネットワーク制御装置１により信号チャネルを介して端末へ伝送される。安全関し、変更ＣＫＣ２に先立ち伝送され且つ古い

暗号鍵で符号化されるがしかし通知されずに（通知なし）のままで．変更ＣＫＣ２後に新たにされた伝送があるときに新たな暗号鍵でデータが符号化されるか否かは重要でない。

【００２４】端末が新たな暗号鍵と共に暗号鍵変更命令ＣＣＣ２を受信後、１つの受取通知命令ＡＣＫ１２のみが無線ネットワーク制御装置１に転送され、それにより．所定の時間期間経過後．無線ネットワーク制御装置１は新たな暗号鍵と共に暗号鍵変更命令ＣＣＣ２を再び送信しない。符号化されるべき各データの転送（アップリンク）も、端末（ＳＴ２２）により停止される。唯一の例外は以下に説明するような新たな暗号鍵で符号化された暗号鍵受取通知命令ＣＣＯＫ２である。暗号鍵受取通知命令ＣＣＯＫ２の伝送後、端末は古い及び新しい暗号鍵の両方でデータを受信し且つ解読（ＣＲ１２）する。暗号鍵変更命令ＣＣＣ２が送信されかつ、受取通知命令ＡＣＫ１２が受信された後、無線ネットワーク制御装置１は、新しい暗号鍵と古い暗号鍵の両方でデータを解読する準備がされている。端末は符号化に間違った新たな暗号鍵を使用したために、無線ネットワーク制御装置１内でのこの命令の解読は有益なないようを提供しない（即ち、無線ネットワーク制御装置は、疑いなしに暗号鍵受取通知命令ＣＣＯＫ２であることを認識できない）場合には．無線ネットワーク制御装置１は端末は誤った新たな暗号鍵が通知されることを認識し得る。古い暗号鍵を伴なうこの暗号鍵受取通知命令ＣＣＯＫ２の解読は．同様に有益な内容を生じない。この第２の誤った符号化結果は．無線ネットワーク制御装置にとって、端末が誤った新たな暗号鍵を知るという更なる確実性を与える。

【００２５】暗号鍵受取通知命令ＣＣＯＫ２の受信は、無線ネットワーク制御装置１により受取通知命令ＡＣＫ２２により端末へ通知される。一方．新たな暗号鍵でのＣＣＯＫ２の解読は、ＣＣＯＫ２が受信されたことを示し．無線ネットワーク制御装置１は再び新たな暗号鍵で．端末とデータ伝送（ダウンリンク）を行う（ＲＴ１２）。受信されたデータは新たな暗号鍵のみでマスクが解除される。無線ネットワーク制御装置１は、端末に新たな暗号鍵で符号化された一致命令ＫＯＫ２を送る。

【００２６】暗号鍵受取通知命令ＣＣＯＫ２が（上述のように）解読できない場合には、再び．古い暗号鍵が受信と送信の両方で使用される（ＲＴ１２／ＣＲ２２）。そして、無線ネットワーク制御装置１は、古い暗号鍵で符号化された一致命令ＫＯＫ２を端末へ送る。この後無線ネットワーク制御装置１は有効なら．他のデータの伝送を回復する。

【００２７】端末と無線ネットワーク制御装置に既知の新たな暗号鍵で暗号の変更を可能とするために．ＲＬＣレイヤはデータ変換手順を行う管理レイヤに知らせ、そして．ここでは説明されないが他の新たな暗号が端末へ通知される。

【００２８】この新たな暗号鍵で符号化された一致命令ＫＯＫ２の受信後、端末は新たな暗号鍵（ＲＴ２２）でデータ伝送（アップリンク）を開始する。これは手順ＣＫＣ２を終了させ、データ転送はこの鍵のみで行われる。

【００２９】古い暗号鍵で符号化されたこの一致命令ＫＯＫ２の受信後．端末は古い暗号鍵でデータ伝送（アップリンク）を回復し、そして、新たな暗号鍵の同時受信が終了される。これは変更ＣＫＣ２を終り停止する。

【００３０】端末は古い暗号鍵と新たな暗号鍵の両方でＣＲ１２とＲＴ２２間で受信されたデータを解読するので．端末は、手順ＣＫＣ２が成功的に終了された（そして端末は新たな暗号鍵で符号化された一致命令ＫＯＫ２を受信し、かつ新たな暗号鍵で解読することは．一致命令ＫＯＫ２が適することを生じ、一方古い暗号鍵で解読することは有益な内容を生じない）か．又は、新たな暗号鍵に変更後の手順は新たに開始されるべきか（そして．端末は古い暗号鍵で符号化された一致命令ＫＯＫ２を受信する：ここで新たな暗号鍵で解読することは有益な内容を生じず．一方、古い暗号鍵で解読することは、ＫＯＫ２が適することを生じるを認識する。これは、間違って受信された鍵の結果として、端末とネットワーク間の全ての接続が遮断されるのを避ける。

【００３１】上述の変更ＣＫＣ２は最初に信号リンクにのみ関連する。データ伝送の繰返しと共に働くデータリンクは、それぞれのレイヤＲＬＣが停止命令（端末：ＳＴ２２、ネットワークＳＴ１２）、又は、ペイロードデータの伝送を回復する命令（端末ＲＴ１２，ネットワークＣＲ２２）が通知される変更中に含まれる。

【００３２】メッセージがレイヤＲＬＣとレイヤＲＲＣ間で伝送される第３の変更ＣＫＣ３を図６から８を参照して説明する。レイヤＲＬＣでは、更に自分及び．インスタンスＲＬＣ（ＤＣ）とＲＬＣ（ＤＴ）間でメッセージが交換される。インスタンスＲＬＣ（ＤＴ）は．専用トラフィックチャネル（ＤＴＣＨ）に対してであり、インスタンスＲＬＣ（ＤＣ）は専用制御チャネル（ＤＣＣＨ）に関してである。

【００３３】暗号鍵変更ＣＫＣ３とともに、無線ネットワーク制御装置１は端末２から９へ新たな暗号鍵の有効性を通知する。この新たな暗号鍵は．無線ネットワーク制御装置１と端末２から９の両方に既知である。図６から８は、端末のレイヤＲＲＣとＲＬＣ（"Ｔ"として参照する図６から８の左側）と、無線ネットワーク制御装置１（"Ｆ"として参照する図６から８の右側）間で送られる種々のメッセージを示す。以後説明する図６は暗号鍵変更ＣＫＣ３の始まりを示す。暗号鍵変更ＣＫＣ３は．サイドＦのレイヤＲＲＣによりローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＤ）により開始される。ローカルメッセージと共にインスタンスＲＬＣ（ＤＣ）は．デー

タユニット中のシリアル番号ＳＮ（各データユニットはシリアル番号が付される）がＳＮ≧ＶＴＤ＋ＮＤの条件を満たす限りメッセージ中のデータユニットの伝送は停止されたことを通知される。ローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＤ）のパラメータＮＤは、そして、まだ伝送されるべきデータユニットの数を示し、そして、ＶＹＤはＲＬＣ（ＤＣ）で既知の伝送されるべき次のデータユニットのシリアル番号を示す。ローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＶＴＤ）により、サイドＦのインスタンスＲＬＣ（ＤＣ）は、シリアル番号ＮＤの受信を知らせ、且つレイヤへ番号ＶＴＤを知らせる。続いて、サイドＦのレイヤＲＲＣは、インスタンスＲＬＣ（ＤＣ）にローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ（ＣＫＮ）を介して使用されるべき新たな暗号鍵ＣＫＮを知らせる。このメッセージは、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃを介してＲＬＣ（ＤＣ）により通知される。

【００３４】インスタンスＲＬＣ（ＤＣ）のレイヤＲＲＣが、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒを配送後、サイドＦのインスタンスＲＬＣ（ＤＣ）は、メッセージＳＥＣ－ＭＯ－ＣＯＭ（ＶＴＤ，ＮＤ）をサイドＴ（端末）のインスタンスＲＬＣ（ＤＣ）へ送る。このメッセージは、安全モード命令を示し、これまで有効な古い暗号鍵で符号化される。メッセージは、番号ＶＴＤとＮＤを伴なうデータユニットを含む。メッセージの受信後、サイドＴのレイヤＲＲＣのインスタンスＲＬＣ（ＤＣ）は、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉを介して、有効であるべき新たな暗号鍵が有効なときから、指示を有するメッセージが到着したことを示す。この新たな暗号鍵は解読を保持する。それはデータユニットのシリアル番号ＶＴＤ＋ＮＤ後である。サイドＴのインスタンスＲＬＣ（ＤＣ）で、メッセージＳＥＣ－ＭＯ－ＣＯＭ（ＶＴＤ，ＮＤ）の受信は、命令ＡＣＫを介してサイドＦのインスタンスＲＬＣ（ＤＣ）から通知され、そして、更にレイヤＲＲＣからローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃを介して通知される。このように無線ネットワーク制御装置１は、端末は暗号鍵変更の最初で通知され且つ条件ＳＮ≧ＶＴＤ＋ＮＤを満たすシリアル番号ＳＮのデータユニットを解読するのに新たな暗号鍵を使用することが通知される。

【００３５】サイドＴ（端末）からの開始で、同様なメッセージの交換が関係のレイヤ間で行われる。サイドＴのレイヤＲＲＣからのローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＵ）は、サイドＴカラのメッセージの交換を開始する。メッセージと共に、条件ＳＮ≧ＶＴＤ＋ＮＵを満たすシリアル番号ＳＮのデータユニットの伝送は、停止される。インスタンスＲＬＣ（ＤＣ）は更に伝送されるべきデータユニットの番号ＮＵが通知される。ローカルメッセージＣＲＬＣ－Ｓ－Ｃ（ＶＴＤ）により、サイドＴのインスタンスＲＬＣ（ＤＣ）は番号ＮＵの受信を通知し、且つレイヤに番号ＶＴＤを示す。ローカルメッセージＣＲＬＣ－Ｓ－Ｃ（ＶＴＤ）の受信後（アップリンクで）最初に送られるこの番号ＶＴＵデータユニットのシリアル番号ＳＮを示す（繰返し伝送はない）。続いて、サイドＴのレイヤＲＲＣは、インスタンスＲＬＣ（ＤＣ）へローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ（ＣＫＮ）を介して鍵を変更することを望むことを知らせる。このメッセージはローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃを介してサイドＴのインスタンスＲＬＣ（ＤＣ）へ通知される。

【００３６】ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒを介して、サイドＴのレイヤＲＲＣから、インスタンスＲＬＣ（ＤＣ）へ、新たな暗号鍵がサイドＴに関して保つときからを示す暗号鍵変更部分が開始される。ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒが受信された後、サイドＴ（端末）のインスタンスＲＬＣ（ＤＣ）は、メッセージＳＥＣ－ＭＯ－ＣＭＰＬ（ＶＴＵ，ＮＵ）をサイドＦ（無線ネットワーク制御装置）のインスタンスＲＬＣ（ＤＣ）へ送る。このメッセージは、安全モード命令を示し、これまで有効な暗号鍵と共に符号化される。メッセージは番号ＶＴＵとＮＵを有するデータユニットを含む。このメッセージの受信後、サイドＦのレイヤＲＲＣのインスタンスＲＬＣ（ＤＣ）は、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉを介して、メッセージが無線ネットワーク制御装置１内で解読のために新たな暗号鍵が有効となるべきときから到着したときを示す。この新たな暗号鍵はデータユニットのシリアル番号ＶＴＵ＋ＮＵ後に有効である。サイドＦのレイヤＲＬＣで、メッセージＳＥＣ－ＭＯ－ＣＭＰＬ（ＶＴＵ，ＮＵ）の受信は、サイドＦのインスタンスＲＬＣ（ＤＣ）の命令ＡＣＫを介して通知され、そして、更にローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃを介してレイヤＲＲＣへ通知される。このように、無線ネットワーク制御装置１は端末がシリアル番号ＶＴＵ＋ＮＵから開始する自身のメッセージのデータユニットを符号化するために新たな暗号鍵を使用することを知っていることが端末に知らされる。

【００３７】図７はプロローグに続いた第１のテスト部分として示される手続の更なる部分を示す。この部分の間は、新たな暗号鍵で符号化された２つのサイドＴとＦのデータユニットからのメッセージ内で正しく符号化され認識される。第１のテスト部分はローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ（ＶＴＵ＋ＮＵ）で開始し、それは、レイヤＲＲＣからインスタンスＲＬＣ（ＤＣ）へサイドＦで伝送される。このように、次のデータユニットのシリアル番号ＳＮに対してＳＮ≧ＶＴＵ＋ＮＵ又は、ＳＮ＝ＶＲの条件が成り立つときには、インスタンスＲＬＣ（ＤＣ）は端末から受信された全てのメッセージは新たな暗号鍵で解読されるべきであることが通知される。ここで、ＶＲは最初に伝送される次の予想される

データユニットを示す。インスタンスＲＬＣ（ＤＣ）は、レイヤＲＲＣへローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃを送ることによりローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ（ＶＴＵ＋ＮＵ）の受信を通知する。サイドＴでは、インスタンスＲＬＣ（ＤＣ）は、レイヤＲＲＣからインスタンスＲＬＣ（ＤＣ）へローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ（ＡＰ）を伝送することにより、このメッセージ後、サイドＦ（無線ネットワーク制御装置１）で伝送されるべき以下のデータユニットが新たな暗号鍵で符号化されることが通知される。しかし、サイドＦの受信されたメッセージは、まだ、古い暗号鍵で解読されるべきである。インスタンスＲＬＣ（ＤＣ）は、サイドＴのレイヤＲＲＣへローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃによりローカルメッセージ ＣＲＬＣ－ＣＯＮＦ－Ｒ（ＡＰ）の受信を通知する。

【００３８】以下のメッセージルーチンと共に、２つのサイドＴとＦが同じ新たな暗号鍵を使用するか否かがチェックされる。このメッセージルーチンはサイドＦのレイヤＲＲＣによりインスタンスＲＬＣ（ＤＣ）へのローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒと共に開始される。このメッセージと共に、サイドＦのインスタンスＲＬＣ（ＤＣ）古い暗号鍵で符号化されたメッセージＳＣＫＣをサイドＴのインスタンスＲＬＣ（ＤＣ）へ送るように要求される。このメッセージＳＣＫＣの受信後、サイドＴのインスタンスＲＬＣ（ＤＣ）は、サイドＦのインスタンスＲＬＣ（ＤＣ）へ受信の通知ＡＣＫを送る。サイドＴのレイヤＲＲＣは、サイドＴのインスタンスＲＬＣ（ＤＣ）へ、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒ内のメッセージＮ（ＣＫＣＣ）を送る。そのメッセージは、サイドＴのインスタンスＲＬＣ（ＤＣ）により複数のデータユニットに分割される。サイドＴのインスタンスＲＬＣ（ＤＣ）は、新たな暗号鍵でこれらのデータを符号化し、そして、サイドＦのインスタンスＲＬＣ（ＤＣ）へそれら（図７のメッセージＣＫＣＣ）を送る。サイドＦのインスタンスＲＬＣ（ＤＣ）は新たな暗号鍵でメッセージＣＫＣＣの全ての受信したデータユニットを解読し、メッセージＣＫＣＣ内で送信されたデータユニットからのメッセージＮ（ＣＫＣＣ）を構築し、そして、サイドＦのレイヤＲＲＣへ、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ＊内でこのメッセージＮ（ＣＫＣＣ）を転送する。ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－ｉ＊は、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ（ＶＴＵ＋ＮＵ）の受信後、最初のデータユニットがシリアル番号ＳＮ＝ＶＲ（これは正確にメッセージＣＫＣＣである）を有するなら、メッセージＮ（ＣＫＣＣ）に関してのみ使用される。この結果、サイドＦのレイヤＲＲＣはインスタンスＲＬＣ（ＤＣ）からメッセージＮ（ＣＫＣＣ）を得ることを知る。

【００３９】サイドＴで、正しい新たな暗号鍵が使用される場合には、サイドのレイヤＲＲＣは、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ＊内に期待するメッセージＮ（ＣＫＣＣ）を受信する。間違った新たな暗号鍵がサイドＴで使用される場合にはサイドＦのレイヤＲＲＣは、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ＊内に、使用できない又は知られていないメッセージを受信する。サイドＦのレイヤＲＲＣは、それから、サイドＴは、間違った鍵を使用した即ち、この特定の場合には知られていないメッセージは無視されないと推定する。

【００４０】メッセージＣＫＣＣの受信後、サイドＦのインスタンスＲＬＣ（ＤＣ）は、サイドＴのインスタンスＲＬＣ（ＤＣ）へ、命令ＡＣＫを介してメッセージＣＫＣＣの受信を通知する。受信はサイドＴのインスタンスＲＬＣ（ＤＣ）により、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃを介してレイヤＲＲＣへ転送される。

【００４１】メッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ＊内に含まれている通信を受信後、サイドＦのレイヤＲＲＣはＴのレイヤＲＲＣへ、サイドＴは正しい新たな暗号鍵を使用したか間違った新たな暗号鍵を使用したか（ＣＫＳＴ＝暗号鍵状態）についての指示を含む、通信Ｎ（ＣＫＳＴ）を送る。サイドＦのレイヤＲＲＣは、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒ内の通信Ｎ（ＣＫＳＴ）をサイドＦのインスタンスＲＬＣ（ＤＣ）へ与るので、これは、順番に起こる。それは、通信を複数のデータユニットに分割し、古い暗号鍵で符号化され、メッセージＣＫＳＴを介してサイドＴのインスタンスＲＬＣ（ＤＣ）へ送る。サイドＴのインスタンスＲＬＣ（ＤＣ）は、メッセージＡＣＫを介してこっちらのデータユニットの受信を通知し、それらを古い暗号鍵で解読し、そして、通信Ｎ（ＣＫＳＴ）を再び再構築する。この通信Ｎ（ＣＫＳＴ）はローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ内でサイドＴのレイヤＲＲＣへ送られる。

【００４２】サイドＴで、正しい新たな暗号鍵が使用される場合には、サイドＦのレイヤＲＲＣは、ローカルメッセージＣＲＬＣ－ＲＥＳ－Ｒを介してインスタンスＲＬＣ（ＤＣ）へ、新たな暗号鍵を使用しながらデータユニットの伝送を再開することを命じる。サイドＦでの解読は受信データユニットのシリアル番号が、ＳＮ≧ＶＴＵ＋ＮＵ成り立つときには、新たな暗号鍵で行われる。

【００４３】メッセージＣＫＳＴがサイドＴで使用された新たな暗号鍵が正しいという通知を含む場合には、サイドＴのレイヤＲＲＣは、ローカルメッセージＣＲＬＣ－ＲＥＳ－Ｒを介してインスタンスＲＬＣ（ＤＣ）へ、新たな暗号鍵を使用しながら再びデータユニットの伝送を開始することを命じる。サイドＴでの解読は、受信データユニットのシリアル番号に、ＳＮ≧ＶＴＤ＋ＮＵ成り立つときには（図７）、新たな暗号鍵で行われる。

【００４４】サイドＴで、誤った新たな暗号鍵が使用されたときには（誤った鍵に対する最初のチェック部を示す図８と比較する）、サイドＦのレイヤＲＲＣは、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒを介してサイド

FのインスタンスＲＬＣ（ＤＣ）へ．条件ＳＮ≧ＶＴＵ＋ＮＵ成り立つときには．解読のための新たな暗号鍵への変換はキャンセルされたことを命じる。伝送が停止されるデータユニットの符号化に対しては、再び古い暗号鍵が使用される。ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒは、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃを介してインスタンスＲＬＣ（ＤＣ）により通知される。ローカルメッセージＣＲＬＣ－ＲＥＳ－Ｒにより、サイドＦのレイヤＲＲＣは．インスタンスＲＬＣ（ＤＣ）へデータユニットの伝送の回復を（古い暗号鍵で）通知する。メッセージＣＫＳＴがサイドＴで使用された新たな暗号鍵が正しくないという支持を含む場合には、サイドＴのレイヤＲＲＣは．ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒを介して．インスタンスＲＬＣ（ＤＣ）へ、条件ＳＮ≧ＶＴＤ＋ＮＵ成り立つときには、解読のための新たな暗号鍵への変換はキャンセルされたことを命令し、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃにより通知される。データユニットがまだ停止しているデータユニットの符号化に関しては．古い暗号鍵が使用される。ローカルメッセージＣＲＬＣ－ＲＥＳ－Ｒにより．サイドＦのレイヤＲＲＣは、インスタンスＲＬＣ（ＤＣ）へデータユニットの伝送を回復することを（古い暗号鍵で）告げる。

【００４５】第４の暗号鍵変更手順ＣＫＣ４を図９から１２により説明する。図９と１０は．端末が正しい新たな暗号鍵を使用し、又は．端末が誤った新たな暗号鍵を使用する場合のそれぞれの場合を示す．暗号鍵変更手順ＣＫＣ４を示す。新たな暗号鍵で符号化及び解読への結果の変換に先立ち、端末が正しい新たな暗号鍵を使用するか否かの第1のチェックが行われるので．エラーの場合には、符号化と解読はサイドＴとＦの間の全ての接続（データ損失なし）が終了されること無く、古い暗号鍵で回復されることができる。以下の手順では、単一の専用のトラフィックチャネルが信号リンク（ＤＣ）に加えて考慮される。従って、一般的には．手順を拡張する、複数の専用のトラフィックチャネルと（手順ＣＫＣのシグナリング目的に使用されない）更なる専用の制御チャネルが可能である。

【００４６】暗号鍵変更手順ＣＫＣ４（図９）は．ローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＣ）又は、ＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＴ）を介してそれぞれサイドＦのレイヤＲＲＣからインスタンスＲＬＣ（ＤＣ）又は．ＲＬＣ（ＤＴ）へ開始される。ローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＣ）又は．ＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＴ）を介してそれぞれ．インスタンスＲＬＣ（ＤＣ）又は．ＲＬＣ（ＤＴ）それぞれは、これまで．データユニットのシリアル番号（各データユニットにはシリアル番号が付される）が、条件ＳＮ≧ＶＴＤ＿ＤＣ＋ＮＤ＿ＤＣ又は、ＳＮ≧ＶＴＤ＿ＤＴ＋ＮＤ＿ＤＴを満たす場合にはデータユニットの伝送が停止されることが通知される。そして．ローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＣ）又は、ＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＴ）のパラメータＮＤ＿ＤＣとＮＤ＿ＤＴはそれぞれ．まだ送信されるべきデータユニットの数を示し、且つ．ＶＴＤ＿ＤＣとＶＴＤ＿ＤＴはそれぞれ．最初に伝送されるべき告ぎのデータユニットのＲＬＣ（ＤＣ）又は．ＲＬＣ（ＤＴ）内で既知のシリアある番号ＳＮである。制御チャネルＤＣに関しては．選択されたＮＤ＿ＤＣは少なくとも非常に大きいので．続くダウンリンクメッセージＳＥＣ－ＭＯ－ＣＮＤとＳＥＣ－ＭＯ－ＫＣ（図９と１０）の全データユニットは．伝送が停止される前に更に送信される。トラフィックチャネルＮＤ＿ＤＴはゼロの設定される。

【００４７】ローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＣ）又はＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＴ）それぞれによって、サイドＦのインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）はそれぞれ、番号ＮＤ＿ＤＣ又はＮＤ＿ＤＴの受信を通知し、且つ番号ＶＴＤ＿ＤＣ又はＶＴＤ＿ＤＴをレイヤに知らせる。続いて．サイドＦのレイヤＲＲＣは、インスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）それぞれに、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ（ＣＫＮ）又はＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ（ＣＫＮ）を介して、使用されるべき新たな暗号鍵ＣＫＮを通知する。このメッセージはサイドＦのインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）それぞれにより、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃ＿ＤＴ又はＣＲＬＣ－ＣＯＮＦ－Ｃ＿ＤＣを介して．通知される。

【００４８】サイドＦのインスタンスＲＬＣ（ＤＣ）は．レイヤＲＲＣから受信されたローカルメッセージＲＬＣ－ＤＡＴ－Ｒ内に含まれる通信ＳＥＣ－ＭＯ－ＣＮＤをサイドＴのインスタンスＲＬＣ（ＤＣ）へ送る。この通信は、安全モード命令を示し、古い今まで有効な鍵で符号化される。１つ又はそれ以上のデータユニットを含む通信は番号ＶＴＤ＿ＤＣ，ＮＤ＿ＤＣ，ＶＴＤ＿ＤＴ及び、ＶＴＤ＿ＤＴを含む。

【００４９】通信の受信後．サイドＴのレイヤＲＲＣのインスタンスＲＬＣ（ＤＣ）は、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉを介して、この通信は新たな暗号鍵が有効となるべきときからの指示を有して到着したことを指示する。この新たな暗号鍵は．データユニットのシリアル番号ＶＴＤ＿ＤＣ＋ＮＤ＿ＤＣから解読するために制御チャネルＤＣ上で前方へ有効であり．シリアル番号ＶＴＤ＿ＤＴ＋ＮＤ＿ＤＴからのトラフィックチャネル上で前方へ有効である。サイドＴのインスタンスＲＬＣ（ＤＣ）通信ＳＥＣ－ＭＯ－ＣＭＤの受信は、サイドのインスタンスＲＬＣ（ＤＣ）の受信通知ＡＣＫを介して、通知され、且つ更に、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃを介してさらにレイヤＲＲＣへ通知される。このように、無線ネットワーク制御装置1に

は、制御チャネルの場合にはシリアル番号ＳＮが条件ＳＮ≧ＶＴＤ＿ＤＣ＋ＮＤ＿ＤＣを満たし、トラフィックチャネルの場合にはシリアル番号ＳＮが条件ＳＮ≧ＶＴＤ＿ＤＴ＋ＮＤ＿ＤＴを満たすときには、端末が暗号鍵変更手順の開始が通知されデータユニットの解読に新たな暗号鍵が使用されるということが、知られている。

【００５０】上述のローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ（ＣＫＮ）とＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＴ（ＣＫＮ）それぞれにより、サイドＦのレイヤＲＲＣはインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）それぞれに、新たな暗号鍵で全ての新たな即ち、繰返しとして送られない期待されるデータユニットを（次の通信が完了するまで）符号化することを命じる。それらは、上述のローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ（ＣＫＮ）とＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＴ（ＣＫＮ）の受信時にシリアル番号が条件ＳＮ≧ＶＲを満たすデータユニットである。ここで、ＶＲはインスタンスＲＬＣ（ＤＣ）で変数であり、次の予想されるデータユニットは繰返しとして送信されないシリアル番号を意味する。

【００５１】サイドＴ（端末）（図１０）の開始からそれぞれのレイヤ間の同様なメッセージの交換が行われる。ローカルメッセージＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＣ）からインスタンスＲＬＣ（ＤＣ）又は、ＣＲＬＣ－Ｓ－Ｒ（ＮＤ＿ＤＴ）からインスタンスＲＬＣ（ＤＴ）それぞれ、サイドＴのレイヤＲＲＣからサイドＴから来るメッセージの交換が開始する。これらの２つのローカルメッセージで、番号が条件ＳＮ≧ＶＴＤ＿ＤＣ＋ＮＤ＿ＤＣ（制御チャネルに対して）及び、ＳＮ≧ＶＴＤ＿ＤＴ＋ＮＤ＿ＤＴ（トラフィックチャネルに対して）を満たすデータユニットの伝送は停止される。そして、まだ伝送されるべきデータユニットの番号ＮＵ＿ＤＣ又は、ＮＵ＿ＤＴは、インスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）へそれぞれ通知される。制御チャネルＤＣに関しては、ＮＵ＿ＤＣは（少なくとも）大きく選択されるべきなので、以下のアップリンク通信ＳＥＣ－ＭＯ－ＫＣ（図１０）とＳＥＣ－ＭＯ－ＣＭＰＬそれぞれ（図１１と１２）は伝送が停止される前に送られる。トラフィックチャネルＮＵ＿ＤＴに関してはゼロに設定される。

【００５２】ローカルメッセージＣＲＬＣ－Ｓ－Ｃ（ＶＴＵ＿ＤＣ）又はＣＲＬＣ－Ｓ－Ｃ（ＶＴＵ＿ＤＴ）により、サイドＴのインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）それぞれは、番号ＮＵ＿ＤＣ又は、ＮＵ＿ＤＴの受信をそれぞれ通知され、そして、レイヤに、番号ＶＴＵ＿ＤＣ又はＶＴＵ＿ＤＴをそれぞれ示す。この番号ＶＴＵ＿ＤＣ又はＶＴＵ＿ＤＴは、それぞれローカルメッセージＣＲＬＣ－Ｓ－Ｃ（ＶＴＵ＿ＤＣ）又はＣＲＬＣ－Ｓ－Ｃ（ＶＴＵ＿ＤＴ）の受信後に、制御チャネル又は、アップリンク内のトラフィックチャネル（繰返し伝送なし）を介して、最初に送信されるデータユニットのシリアル番号ＳＮを示す。続いて、サイドＴのレイヤＲＲＣは、インスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）それぞれにローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ（ＣＫＮ）又は、ＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＴ（ＣＫＮ）を介して、それぞれ、暗号鍵の変更の希望を通知する。番号ＶＴＤ＿ＤＣ＋ＮＤ＿ＤＣにより、ＶＴＤ＿ＤＴ＋ＮＤ＿ＤＴは、さらに、そこから前方へ新たな暗号鍵で解読が行われる。データユニットのシリアル番号が通知される。各々がローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃ＿ＤＣ又はＣＲＬＣ－ＣＯＮＦ－Ｃ＿ＤＣを伴なう、このローカルメッセージは、サイドＴのインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）により通知される。

【００５３】インスタンスＲＬＣ（ＤＣ）へのサイドＴのレイヤＲＲＣのローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒ＊により、手順部分は開始し、それによりサイドＦは、サイドＴは正しい新たな暗号鍵を使用するか否かをチェックできる。ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒ＊の受信後、サイドＴ（端末）のインスタンスＲＬＣ（ＤＣ）は、通信ＳＥＣ－ＭＯ－ＫＣをサイドＦ（無線ネットワーク制御装置1）のインスタンスＲＬＣ（ＤＣ）へ送り、新たな暗号鍵で符号化される。上記場合のアステリスク（"＊"）は、（例えば、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒ内の更なるパラメータ（フラグ）により）、インスタンスＲＬＣ（ＤＣ）が、この特定の通信に対して符号化に新たな暗号鍵が使用されるべきであることが示されていることを意味する。

【００５４】サイドＦのインスタンスＲＬＣ（ＤＣ）でメッセージのデータユニットのシリアル番号が条件ＳＮ≧ＶＲを満たし、それによりそれらは新たな暗号鍵で解読される。新たな暗号鍵で解読されたデータユニットからの再構成されたメッセージは、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ＊と共にサイドＦのレイヤＲＲＣへ与えられ、一方上記場合のアステリスク（"＊"）は、（例えば、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ内の更なるパラメータ（フラグ）により）、ＲＲＣが、パラメータとして伝送された通信が新たな暗号鍵で解読されるデータユニットの組合せであることを示されることを意味する。正しい鍵の信頼あるチェックのために、通信ＳＥＣ－ＭＯ－ＫＣに、複数のデータユニットよりなることが必要である。

【００５５】サイドＦのレイヤＲＲＣはこの時点で通信ＳＥＣ－ＭＯ－ＫＣを期待する。サイドＴで正しい新たな暗号鍵が符号化に使用される場合には、レイヤＲＲＣはローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉ＊のパラメータ内のこの通信を認識し、且つ図１０と１１に記載されたように手順が行う。

【００５６】サイドＴで新たな間違った暗号鍵が符号化

に使用される場合には、レイヤＲＲＣはローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－ｉ＊のパラメータ内の通信は有益又は既知でないと認識する。この特定の場合、知られていない通信がローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－ｉ＊と共にレイヤＲＲＣにより受信された場合には、レイヤＲＲＣはこの知られていない通信を単純に拒絶せず、しかし、サイドＴは間違った新たな暗号鍵を使用していると認識する。この場合は、手続は図１２に示すように継続する。

【００５７】両場合には、サイドＦのレイヤＲＲＣは（インスタンスＲＬＣ（ＤＣ）へのローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒのパラメータとして）、サイドＴで、通信ＳＥＣ－ＭＯ－ＫＣＳＴを送る。それは、サイドＦのレイヤＲＲＣが確立されたか否か、サイドＴは正しい新たな暗号鍵又は誤った新たな暗号鍵を使用しているかの指示を含む。通信ＳＥＣ－ＭＯ－ＫＣＳＴのデータユニットは、常に古い暗号鍵で符号化される。

【００５８】以下は図１１に示す通常の場合である。サイドＦのインスタンスＲＬＣ（ＤＣ）へ、サイドＦの通信ＳＥＣ－ＭＯ－ＫＣＳＴの受信に関して、サイドＴのインスタンスＲＬＣ（ＤＣ）により受信の通知ＡＣＫを転送する、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃの受信後、サイドＦのレイヤＲＲＣはローカルメッセージＣＲＬＣ－ＲＥＳ－Ｒ＿ＤＣ又はＣＲＬＣ＿ＲＥＳ＿Ｒ＿ＤＴを介して、インスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）へ、インスタンスＲＬＣ（ＤＣ）内のシリアル番号ＳＮが条件ＳＮ≧ＶＴＤ＿ＤＣ＋ＮＤ＿ＤＣを満たし又は、インスタンスＲＬＣ（ＤＴ）内で条件ＳＮ≧ＶＴＤ＿ＤＴ＋ＮＤ＿ＤＴを満たす今まで停止されていたデータユニットの伝送を開始するように命じる。これらのデータユニットは新たな暗号鍵で符号化される。

【００５９】以下の図１２に示すエラーの場合が記述される。レイヤＲＲＣへ、サイドＦの通信ＳＥＣ－ＭＯ－ＫＣＳＴの受信に関して、サイドＴのＲＬＣ（ＤＣ）の受信の通知ＡＣＫを転送する、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃが受信された後、サイドＦのレイヤＲＲＣは以後説明する更なるメッセージの後に、最初にローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ又はＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＴそれぞれにより、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｃ＿ＤＣ又ＣＲＬＣ－ＣＯＮＦ－Ｃ＿ＤＴにより通知される、新たな暗号鍵の変換をキャンセルすることを命じ、続いてローカルメッセージＣＲＬＣ－ＲＥＳ－Ｒ＿ＤＣ又はＣＲＬＣ－ＲＥＳ－Ｒ＿ＤＴにより、レイヤＲＬＣ（ＤＣ）内のシリアル番号ＳＮが、条件ＳＮ≧ＶＴＤ＿ＤＣ＋ＮＤ＿ＤＣ又は、ＲＬＣ（ＤＴ）内のシリアル番号ＳＮが、条件ＳＮ≧ＶＴＤ＿ＤＴ＋ＮＤ＿ＤＴを満たす今まで停止してデータユニットの伝送を回復することを命じる。これらのデータユニットは古い暗号鍵で符号化される。

【００６０】受信の通知ＡＣＫの結果、サイドＦの通信ＳＥＣ－ＭＯ－ＫＣの受信はＴ（図１０）へ通知される。ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃはこの通知をサイドＴ上のレイヤＲＲＣへ伝送する。通知の受信後、サイドＴはサイドＦからの通信ＳＥＣ－ＭＯ－ＫＣＳＴを期待する（図１１及び１２）。インスタンスＲＬＣ（ＤＣ）での通信ＳＥＣ－ＭＯ－ＫＣＳＴの受信の時は、その受信はサイドＦへ通信ＡＣＫを介して通知され、サイドＴのこのインスタンスは通信ＳＥＣ－ＭＯ－ＫＣＳＴをローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－ＩのパラメータとしてサイドＴのレイヤＲＲＣへ渡す。

【００６１】通常の場合（図１１）にサイドＴの通信ＳＥＣ－ＭＯ－ＫＣＳＴが使用される新たな暗号鍵が正しい新たな暗号鍵を示す場合には、サイドＴは通信ＳＥＣ－ＭＯ－ＣＭＰＬをサイドＦへ送る。ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒ（図１１）の受信後、サイドＴ（端末）のインスタンスＲＬＣ（ＤＣ）は通信ＳＥＣ－ＭＯ－ＣＭＰＬをサイドＦ（無線ネットワーク制御装置）のインスタンスＲＬＣ（ＤＣ）へ送る。この通信は安全モード命令を示し、且つそれまで有効な古い暗号鍵で符号化される。メッセージは１つ又はそれ以上のデータユニットからなり、番号ＶＴＵ＿ＤＣ，ＮＵ＿ＤＣ，ＶＴＵ＿ＤＴ及び、ＮＵ＿ＤＴを転送する。通信の受信後、サイドＦのレイヤＲＲＣのインスタンスＲＬＣ（ＤＣ）は、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｉを介して、この通信は、無線ネットワーク制御装置内の解読に関して新たな暗号鍵が有効であるべき時からの指示と共に到着したことを示す。この新たな暗号鍵は、シリアル番号ＳＮが、条件ＳＮ≧ＶＴＵ＿ＤＣ＋ＮＵ＿ＤＣ（制御チャネル）又は、条件ＳＮ≧ＶＴＵ＿ＤＴ＋ＮＵ＿ＤＴ（トラフィックチャネル）を満たすデータユニットを表す。

【００６２】通信ＳＥＣ－ＭＯ－ＣＭＰＬの受信後、Ｆのレイヤ ＲＲＣはインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）に、ローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ又はＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＴにより、シリアル番号ＳＮが、インスタンスＲＬＣ（ＤＣ）では条件ＳＮ≧ＶＴＵ＿ＤＣ＋ＮＵ＿ＤＣ又は、インスタンスＲＬＣ（ＤＴ）では条件ＳＮ≧ＶＴＵ＿ＤＴ＋ＮＵ＿ＤＴ（トラフィックチャネル）を満たす全てのデータユニットを解読するための新たな暗号鍵を使用することを命じる。

【００６３】サイドＦのインスタンスＲＬＣ（ＤＣ）で通信ＳＥＣ－ＭＯ－ＣＭＰＬは、サイドＴのインスタンスＲＬＣ（ＤＣ）の受信の通知ＡＣＫを介して通知され、且つ更に、それらのレイヤＲＲＣはローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃを介して通知される。このように、端末には、無線ネットワーク制御装置１には端末が、制御チャネル上のシリアル番号ＶＴＵ＿ＤＣ＋

ＮＵ＿ＤＣから前方へ及び．トラフィックチャネル上のＶＴＵ＿ＤＴ＋ＮＵ＿ＤＴから、新たな暗号鍵を自己の通信のデータユニットの符号化に対して使用することを知っているということを知る。

【００６４】サイドＴは正しい新たな暗号鍵を使用するので．それらのレイヤＲＲＣはインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）へ．ローカルメッセージＣＲＬＣ－ＲＥＳ－Ｒ＿ＤＣ又はＣＲＬＣ－ＲＥＳ－Ｒ＿ＤＴ（図１１）を介して、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃ受信後、シリアル番号ＳＮが、制御チャネルに対してはインスタンスＲＬＣ（ＤＣ）で条件ＳＮ≧ＶＴＵ＿ＤＣ＋ＮＵ＿ＤＣ又は、トラフィックチャネルに対してはインスタンスＲＬＣ（ＤＴ）では条件ＳＮ≧ＶＴＵ＿ＤＴ＋ＮＵ＿ＤＴを満たす今まで停止されたデータユニットの伝送を回復するように命じる。

【００６５】サイドＴの通信ＳＥＣ－ＭＯ－ＫＣＳＴが使用される新たな暗号鍵が間違い（誤り）（図１２）であることを示すときには．レイヤＲＲＣは、インスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）に、２つのローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣとＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＴにより、新たな暗号鍵の変換を停止するように命じる。

【００６６】さらに、サイドＴは通信ＳＥＣ－ＭＯ－ＣＭＰＬを、サイドＦへ手順を終了するために送る。この通信は、ローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｒのパラメータとして、無線インターフェースを介してサイドＦのインスタンスＲＬＣ（ＤＣ）へ与えられ．このインターフェースによりローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－ＩのパラメータとしてッサイドＦのレイヤＲＲＣへ与えられる。新たな暗号鍵の使用は切り替えがつづいていないので、メッセージＳＥＣ－ＭＯ－ＣＭＰＬは．番号ＶＴＵ＿ＤＣ．ＮＵ＿ＤＣ．ＶＴＵ＿ＤＴ及び．ＮＵ＿ＤＴを含む必要がない。

【００６７】解読に関しては、サイドＦのインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）でなにも変更が起こらず．解読のためにこれらのインスタンスに関して再コンフィグレーションはいずれも必要で無く、それにより暗号鍵変更ＣＫＣは，サイドＦのエラーの場合には、通信ＳＥＣ－ＭＯ－ＣＭＰＬの受信で終了する。

【００６８】サイドＴのインスタンスＲＬＣ（ＤＣ）の通信ＳＥＣ－ＭＯ－ＣＭＰＬに対する受信の通知ＡＣＫ後に．それはサイドＴのレイヤＲＲＣへローカルメッセージＲＬＣ－ＡＭ－ＤＡＴ－Ｃを介して伝送される。サイドＴのレイヤＲＲＣはそして、インスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）へ、２つのローカルメッセージＣＲＬＣ－ＲＥＳ－Ｃ＿ＤＣ又は．ＣＲＬＣ－ＲＥＳ－Ｃ＿ＤＴにより、シリアル番号ＳＮが、制御チャネルに対してはインスタンスＲＬＣ（ＤＣ）で条件ＳＮ≧ＶＴＵ＿ＤＣ＋ＮＵ＿ＤＣ又は、トラフィックチャネルに対してはインスタンスＲＬＣ（ＤＴ）では条件ＳＮ≧ＶＴＵ＿ＤＴ＋ＮＵ＿ＤＴを満たす今まで停止されたデータユニットの伝送を回復するように命じる。

【００６９】新たな暗号鍵への変更は前にインスタンスＲＬＣ（ＤＣ）で２つのローカルメッセージＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＣ及びインスタンスＲＬＣ（ＤＴ）でＣＲＬＣ－ＣＯＮＦ－Ｒ＿ＤＴを介してキャンセルされているので、これらのデータユニットは、古い暗号鍵で符号化される。エラーの場合には、暗号鍵変更はサイドＴで終わる。

【００７０】第５の暗号鍵変更手順ＣＫＣ５を１３と１４により説明する。前述のように、レイヤＲＬＣとレイヤＲＲＣ間のローカルメッセージはこの手順中に伝送される。レイヤＲＬＣは２つのインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）を利用できる。インスタンスＲＬＣ（ＤＴ）は専用トラフィックチャネル（ＤＴＣＨ）を制御でき、或Ｔインスタンスは、ＲＬＣ（ＤＣ）は専用制御チャネル（ＤＣＣＨ）を制御できる。端末は例えば、ＧＳＭ（" ＧＳＭ移動通信のためのグローバルシステム" Ｊ．ＥｂｅｒｓｐａｃｈｅｒとＨ．Ｊ．Ｖｏｇｅｌ、ＴｅｕｂｎｅｒＳｔｕｔｔｇａｒｔ１９９７年１４６頁から１５４頁参照）で説明されているように端末と無線ネットワーク制御装置の間の別の貧小手順で新たな暗号鍵についての情報を受信する。この文献中では、鍵それ自身は無線インターフェースを介して伝送される。

【００７１】記述されるべき手順ＣＫＣ５で、端末と無線ネットワーク制御装置間の古い暗号鍵から新たな暗号鍵への同期した変換が行われる。手順ＣＫＣ５は．プローグフェーズで始まり．同期フェーズが続く。図１３と１４は、端末のレイヤＲＲＣとレイヤＲＬＣ（図４と５の左側を" Ｔ" と呼ぶ）と無線ネットワーク制御装置（図４と５の右側を" Ｆ" と呼ぶ）間で送られる種々のメッセージを示す。

【００７２】最初に、（図４と比較して）無線ネットワーク制御装置１は、端末に新たな暗号鍵の意図された変更を通知する。サイドＦでは、レイヤＲＲＣは．インスタンスＲＬＣ（ＤＣ）へローカルメッセージＡＭＤ－ＲＥＱ－ＣＣＣにより通信ＡＭＤ－ＰＤＵ－ＣＣＣをサイドＴのインスタンスＲＬＣ（ＤＣ）へ送るように命じる。このインスタンスは．サイドＦのインスタンスＲＬＣ（ＤＣ）へ通知を介して受信ＡＣＫを知らせ．サイドＴのレイヤＲＲＣにローカルメッセージＡＭＤ－ＲＥＱ－ＣＣＣＣを介して受信された通信を知らせる。サイドＦでは、受信の通知ＡＣＫがインスタンスＲＬＣ（ＤＣ）によりレイヤＲＲＣへローカルメッセージＡＭＤ－ＣＯＮ－ＣＣＣを介して送る。

【００７３】サイドＴでは．レイヤＲＲＣは、インスタンスＲＬＣ（ＤＣ）へローカルメッセージＡＭＤ－ＲＥＱ－ＣＣＯＫを介して、通信ＡＭＤ－ＰＤＵ－ＣＣＯＫをサイドＦのインスタンスＲＬＣ（ＤＣ）へ送る。サイドＦのインスタンスＲＬＣ（ＤＣ）はサイドＴのインス

タンスＲＬＣ（ＤＣ）へ受信の通知ＡＣＫを介して通知し．そして、サイドＦのレイヤＲＲＣへ、受信された通信を介してローカルメッセージＡＭＤ－ＩＮＤ－ＣＣＯＫを介して送る。サイドＴでは、受信の通知ＡＣＫがインスタンスＲＬＣ（ＤＣ）によりレイヤＲＲＣへローカルメッセージＡＭＤ－ＣＯＮ－ＣＣＯＫを介して転送される。

【００７４】今まで説明したメッセージと通信の交換は．手順ＣＫＣ５のプロローグとして参照される。通信ＡＭＤ－ＰＤＵ－ＣＣＣとＡＭＤ－ＰＤＵ－ＣＣＯＫは．古い暗号鍵で符号化される。これらの通信はＲＬＣヘッダと呼ばれる制御情報を伴なう制御部を有する。ＲＬＣヘッダの特別ビットC_kは、新たな暗号鍵又は古い暗号鍵のいずれかが使用されるのかを示す。この特別ビットC_kを使用するときには、手順ＣＫＣ５に先立ち一度既に伝送され且つその受信がまだ通知されていないデータユニットは古い暗号鍵と共に再度転送されることができることが可能である。プロローグ後に最初に送信されるときにはデータユニットは新たな暗号鍵で送信される。この手段は．繰返し伝送の場合には、聴者は．伝送の繰返しのフェーズ中にチャネルを聞く場合には．常に既に受信された符号化されたデータユニットと同一のコピーを聞き且つ新たな情報を何も受信しない。

【００７５】手順ＣＫＣ５のプロローグの前に．特別ビットC_kがゼロに設定される。特別ビットC_kが１に設定された後、次の同期フェーズで、データが新たな暗号鍵で符号化されることを示し、一方．同期フェーズで０に設定されたビットC_kは．データが古い暗号鍵で符号化されることを示す。

【００７６】同期フェーズは端末と無線ネットワーク制御装置で異なる時間に開始し、：ダウンリンク（ＤＬ）では同期フェーズは、ローカルメッセージＳＴＡＲＴ－ＣＫＣＳ－ＤＬ及びＳＴＡＲＴ－ＣＫＣＳ－ＤＴ同期フェースの開始のレイヤＲＬＣのレイヤＲＲＣがインスタンスＲＬＣ（ＤＣ）又はＲＬＣ（ＤＴ）に通知した後、第1のデータユニットＤＬ－ｎｅｗ－ｎｅｗの伝送と共に開始する。（ダウンリンクで送られた）データユニットは．プロローグ後の最初に伝送されたとき、ＤＬ－ｎｅｗ－ｎｅｗと呼ばれる。データユニットＤＬ－ｎｅｗ－ｎｅｗは、伝送の繰返しが起こるとすぐにデータユニットＤＬ－ｎｅｗとなる。データユニットは（最初に又は繰返しとして）プロローグ前に既に伝送されていれば．ＤＬ－ｏｌｄ－ｏｌｄと呼ばれる。データユニットは．プロローグ後に再び伝送されるときには、ＤＬ－ｏｌｄと呼ばれる。

【００７７】アップリンク（ＵＬ）では、同期フェーズは最初のデータユニットＵＬ－ｎｅｗ－ｎｅｗの伝送で開始する。（アップリンクで送られた）データユニットは．最初のでーユニットＤＬ－ｎｅｗ－ｎｅｗ又はＤＬ－ｎｅｗ後の最初に伝送されたとき．ＤＬ－ｎｅｗ－ｎｅｗと呼ばれる。データユニットＤＬ－ｎｅｗ－ｎｅｗは．再び伝送されるとすぐにデータユニットＵＬ－ｎｅｗとなる。データユニットは、最初のデータユニットＤＬ－ｎｅｗ－ｎｅｗ又はＤＬ－ｎｅｗの繰返し前に既に伝送されていれば、ＵＬ－ｏｌｄ－ｏｌｄと呼ばれる。それは、最初のデータユニットＤＬ－ｎｅｗ－ｎｅｗ又はＤＬ－ｎｅｗの繰返し後にデータユニットＤＬ－ｏｌｄ－ｏｌｄが繰返し伝送される場合には、データユニットＵＬ－ｏｌｄと呼ばれる。

【００７８】以下の規則１から５は．同期フェーズを制御し．特別のビットC_kはゼロに設定され、アップリンクとダウンリンクの両方の後にそれぞれのデータユニットは新たな暗号鍵のみで符号化され．全データユニットＵＬ－ｏｌｄとＤＬ－ｏｌｄはいずれか成功的に（古い暗号鍵で符号化され）伝送され又は．伝送の許された繰返しの最大数はこれらのデータユニットに達する。最大数に達したときに、これらのデータユニットを伝送するのに更なる労力は成されない。

【００７９】規則１：ダウンリンクの同期フェーズ中に．サイドＦのレイヤＲＬＣ（例えば．インスタンスＲＬＣ（ＤＣ））は、新たな暗号鍵で符号化したデータユニットＤＬ－ｎｅｗ－ｎｅｗ及びＤＬ－ｎｅｗを送る。特別ビットC_kは１に設定されている。一方データユニットＤＬ－ｏｌｄは、特別ビットC_kが０に設定されている間は、古い暗号鍵で符号化し送られる。図１４では．そのようなデータユニットはデータユニット番号２６を有する。アップリンクの同期フェーズ中は．レイヤＲＬＣ（例えば．インスタンスＲＬＣ（ＤＴ））は、特別ビットC_kが１に設定されている間は、新たな暗号鍵で符号化したデータユニットＤＬ－ｎｅｗ－ｎｅｗ及びＤＬ－ｎｅｗ送る。データユニットＤＬ－ｏｌｄは、特別ビットC_kが０に設定されている間は、古い暗号鍵で符号化し送られる。

【００８０】規則２：レイヤＲＬＣは．エラーなしに受信された最初のデータユニットＤＬ－ｎｅｗ－ｎｅｗ及びＤＬ－ｎｅｗの連続のデータユニット番号ＳＮ（シーケンス番号）を蓄積する。このデータユニット番号は、ＲＬＣヘッダの一部を構成し、かつサイドＴのＳＮ$_{P-DL}$（Ｔ）と呼ばれる。

【００８１】図１４では．SN_{P-DL}（Ｔ）は．データユニット番号２８を有する。シーケンス番号２７を有する（図１４）前に送られたデータユニットＤＬ－ｎｅｗ－ｎｅｗは．エラーなしに送られない。シーケンス番号２７を有するデータユニットが再び送られるとき、このデータユニットはＤＬ－ｎｅｗとなる。

【００８２】サイドＦのレイヤＲＬＣは、最初に通知されたデータユニットＤＬ－ｎｅｗ－ｎｅｗ及びＤＬ－ｎｅｗの連続のデータユニット番号ＳＮを蓄積する。このデータユニット番号は、SN_{P-DL}（Ｆ）と呼ばれる。図１４では．SN_{P-DL}（Ｆ）は、データユニッ

ト番号２８を有し且つデータユニットＤＬ－ｎｅｗ－ｎｅｗに属する。

【００８３】規則３：サイドＦのレイヤＲＬＣは、エラーなしに受信された最初のデータユニットＵＬ－ｎｅｗ－ｎｅｗ及びＵＬ－ｎｅｗの連続の番号ＳＮ（シーケンス番号）を蓄積する。この番号は、$SN_{F-UL}(F)$と呼ばれる。図１４では、それは、データユニット番号５４を有し、データユニットＵＬ－ｎｅｗ－ｎｅｗより来る。一方データユニット番号５３を有するデータユニットはデータユニットＵＬ－ｏｌｄである。一般的に以下が成り立つ。

$SN_{F-DL}(T) \leq SN_{F-DL}(F)$及び、

$SN_{F-UL}(F) \leq SN_{F-UL}(T)$。

【００８４】これらのデータユニット番号$SN_{F-DL}(T)$、$SN_{F-DL}(F)$、$SN_{F-UL}(F)$、$SN_{F-UL}(T)$はプロローグフェーズ中は無効値が与えられる。データユニットのＲＬＣヘッダから得たデータユニット番号は有効値である。

【００８５】規則４：$SN_{F-UL}(F)$が有効値を得たときのみ、ダウンリンク内の同期フェーズは終了されることができる。サイドＦのレイヤＲＬＣが全データユニットＤＬ－ｏｌｄとＤＬ－ｎｅｗに関する通知を受信する、又は、全データユニットＤＬ－ｏｌｄとＤＬ－ｎｅｗの伝送の繰返しの最大数に達すると終了される。サイドＦのレイヤＲＬＣはいつでもダウンリンク上で送信された全てのデータユニットを知っているので、この判断ができる。ダウンリンクの同期フェーズの終了は、メッセージＥＮＤ－ＣＫＣＳ－ＤＬ－Ｆを介してサイドＦのレイヤＲＲＣへ通知される。

【００８６】ダウンリンク内の同期フェーズの終了は、サイドＴで示され、特別ビットC_kがゼロに設定されたデータユニットＤＬ－ｎｅｗ－ｎｅｗが送られ、しかし新たな暗号鍵で符号化される。図１４では、これと同様に送られる最初のデータユニットは、データユニット番号２９を有する。サイドＴのレイヤＲＬＣは、特別ビットC_kがゼロに設定され受信されたデータユニットのデータユニット番号が、蓄積値$SN_{F-DL}(T)$より大きいか又は等しいことからダウンリンク内の同期フェーズの終了を認識する。

【００８７】ダウンリンク内の同期フェーズの終了後、サイドＦのレイヤＲＬＣは新たな暗号鍵と特別ビットC_kがゼロに設定されて符号化された全データユニットを送る。サイドＴのレイヤＲＬＣは、新たな暗号鍵で符号化されたデータユニットを受信する。

【００８８】規則５：サイドＴのレイヤＲＬＣは、全データユニットＤＬ－ｏｌｄとＤＬ－ｎｅｗが通知され又は、これらのデータユニットに対する伝送の繰返しの最大数に達することにより、アップリンク内の同期フェーズの終了を認識する。アップリンク内の同期フェーズの終了は、メッセージＥＮＤ－ＣＫＣＳ－Ｔを介してサイドＴのレイヤＲＲＣへ通知される。

【００８９】アップリンクの同期フェーズの終了は、特別ビットC_kがゼロに設定されたデータユニットＤＬ－ｎｅｗ－ｎｅｗが送られ、しかし新たな暗号鍵で符号化され、サイドＦに示される。図１４では、これと同様の最初のデータユニットはデータユニット番号５５である。サイドＦのレイヤＲＬＣは、特別ビットC_kがゼロに設定され受信されたデータユニットのデータユニット番号が、蓄積値$SN_{F-UL}(F)$より大きいか又は等しいことからアップリンクの同期フェーズの終了を認識する。アップリンクの同期フェーズの終了は、メッセージＥＮＤ－ＣＫＣＳ－Ｆを介してサイドＦのレイヤＲＲＣへ通知され、それにより新たな手順ＣＫＣＳが再び開始される。

【００９０】アップリンクの同期フェーズの終了後、サイドＴのレイヤＲＬＣ層は、新たな暗号鍵と特別ビットC_kがゼロに設定された符号化の形式で全データユニットを送る。そして、サイドＦのレイヤＲＬＣは、新たな暗号鍵で符号化されたデータユニットのみを受信する。

【００９１】特別ビットC_kを使用することにより、手順ＣＫＣＳは伝送のどのような中断も発生しないことが達成される。蓄積値$SN_{F-DL}(T)$、$SN_{F-DL}(F)$、$SN_{F-UL}(F)$、$SN_{F-UL}(T)$を使用することなしに、手順ＣＫＣＳをエラーなしで終了させることができない。

【００９２】

【発明の効果】本発明により、異なる暗号変更手順を有する無線ネットワークを提供することできる。

【図面の簡単な説明】

【図１】無線ネットワーク制御装置と複数の端末を有する無線ネットワークを示す図である。

【図２】端末又は無線ネットワーク制御装置の種々の機能を説明するためのレイヤモデルを示す図である。

【図３】端末又は無線ネットワーク制御装置の符号化機構を説明するためのフロック図である。

【図４】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図５】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図６】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図７】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図８】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図９】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

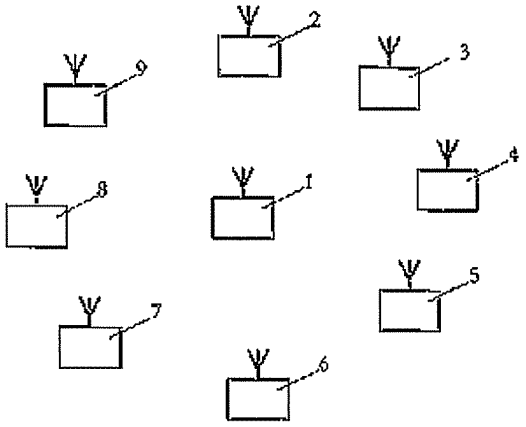
【図１０】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図１１】符号化に必要な暗号鍵を変更する手順中の種

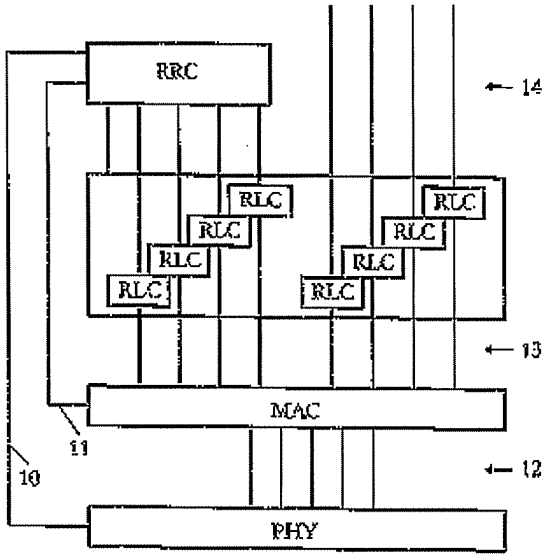
ｙの命令のルーチンを示す図である。
【図１２】符号化に必要な暗号鍵を変更する手順中の種ｙの命令のルーチンを示す図である。
【図１３】符号化に必要な暗号鍵を変更する手順中の種ｙの命令のルーチンを示す図である。
【図１４】符号化に必要な暗号鍵を変更する手順中の種＊ｙの命令のルーチンを示す図である。

【符号の説明】
１　無線ネットワーク制御装置
２から９　端末
１６　符号化機能

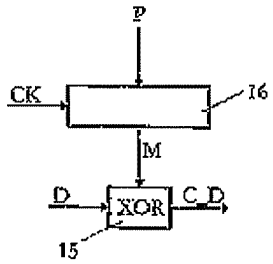
【図１】



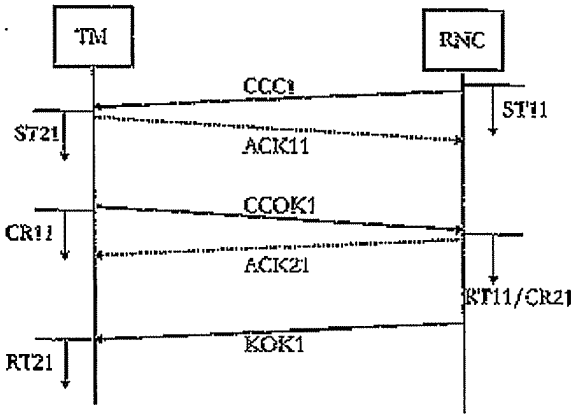
【図２】



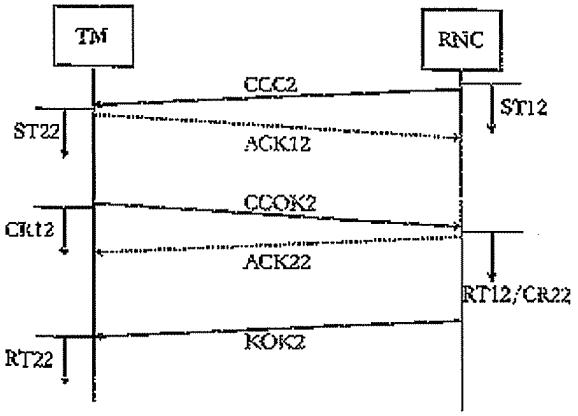
【図３】



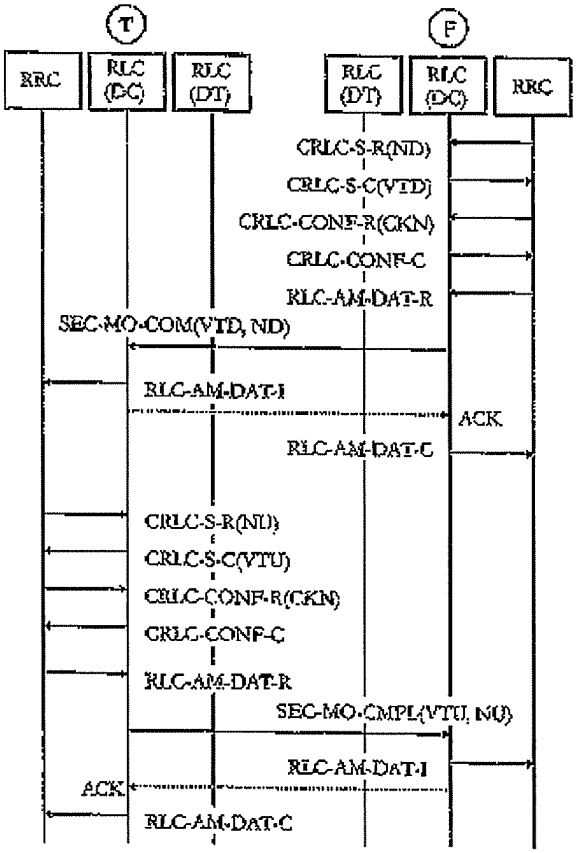
【図４】



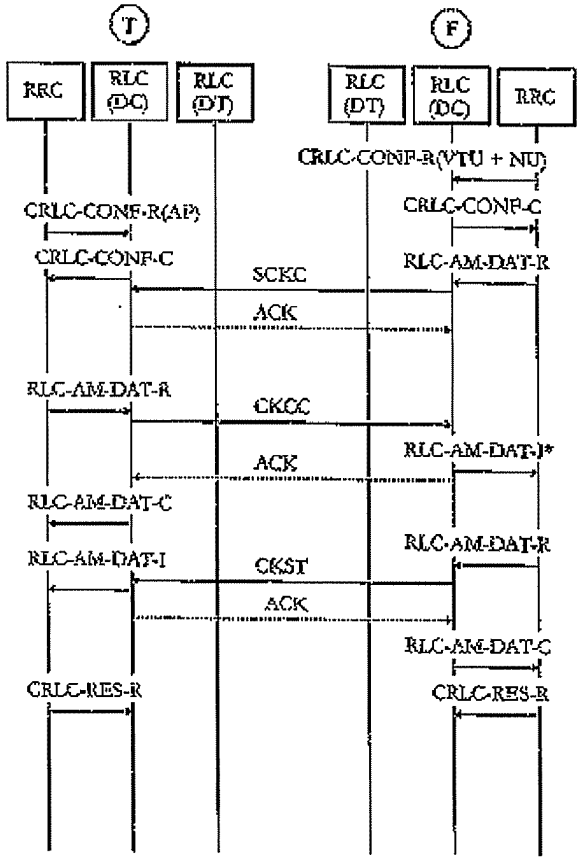
【図５】


TM
RNC
CCC2
ST12
ST22
ACK12
CCOK2
CR12
ACK22
RT12/CR22
KOK2
RT22

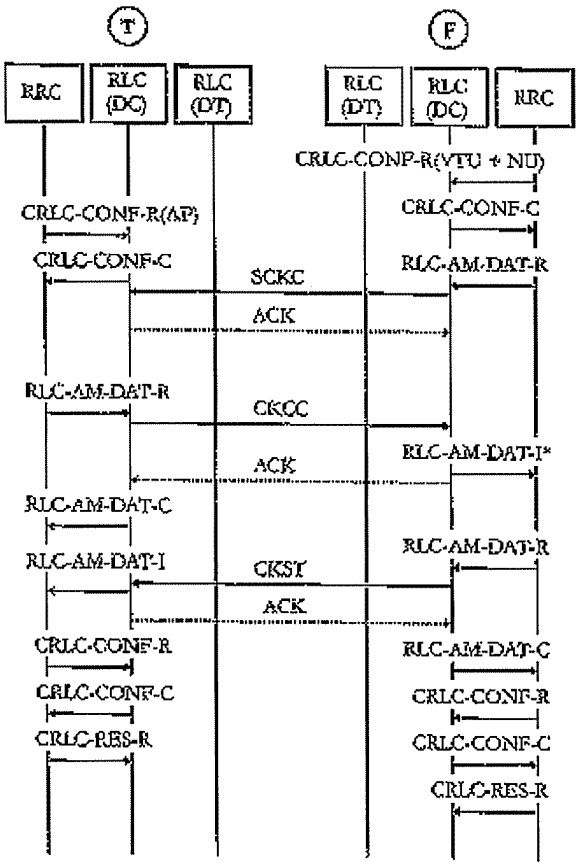
【図６】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
CRLC-S-R(ND)
CRLC-S-C(VTD)
CRLC-CONF-R(CKN)
CRLC-CONF-C
RLC-AM-DAT-R
SEC-MO-COM(VTD, ND)
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C
CRLC-S-R(NU)
CRLC-S-C(VTU)
CRLC-CONF-R(CKN)
CRLC-CONF-C
RLC-AM-DAT-R
SEC-MO-CMPL(VTU, NU)
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C

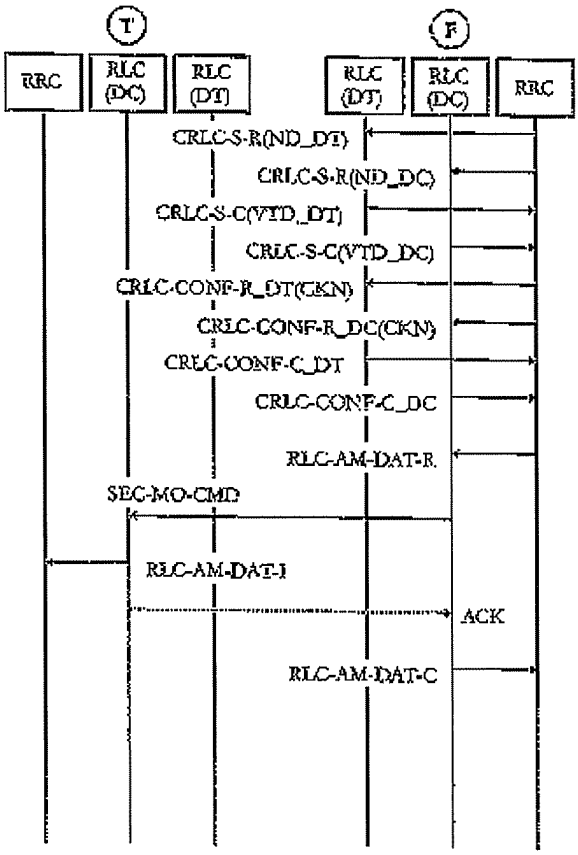
【図７】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
CRLC-CONF-R(VTU + NU)
CRLC-CONF-R(AP)
CRLC-CONF-C
CRLC-CONF-C
RLC-AM-DAT-R
SCKC
ACK
RLC-AM-DAT-R
CKCC
RLC-AM-DAT-I*
ACK
RLC-AM-DAT-C
RLC-AM-DAT-R
RLC-AM-DAT-I
CKST
ACK
RLC-AM-DAT-C
CRLC-RES-R
CRLC-RES-R

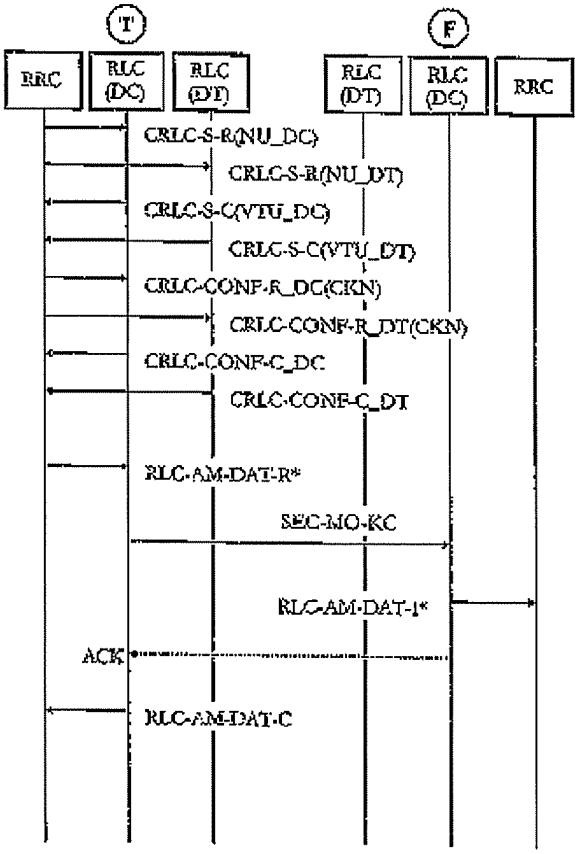
【図８】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
CRLC-CONF-R(VTU + NU)
CRLC-CONF-R(AP)
CRLC-CONF-C
CRLC-CONF-C
SCKC
RLC-AM-DAT-R
ACK
RLC-AM-DAT-R
CKCC
ACK
RLC-AM-DAT-I*
RLC-AM-DAT-C
RLC-AM-DAT-I
CKST
RLC-AM-DAT-R
ACK
CRLC-CONF-R
RLC-AM-DAT-C
CRLC-CONF-C
CRLC-CONF-R
CRLC-RES-R
CRLC-CONF-C
CRLC-RES-R

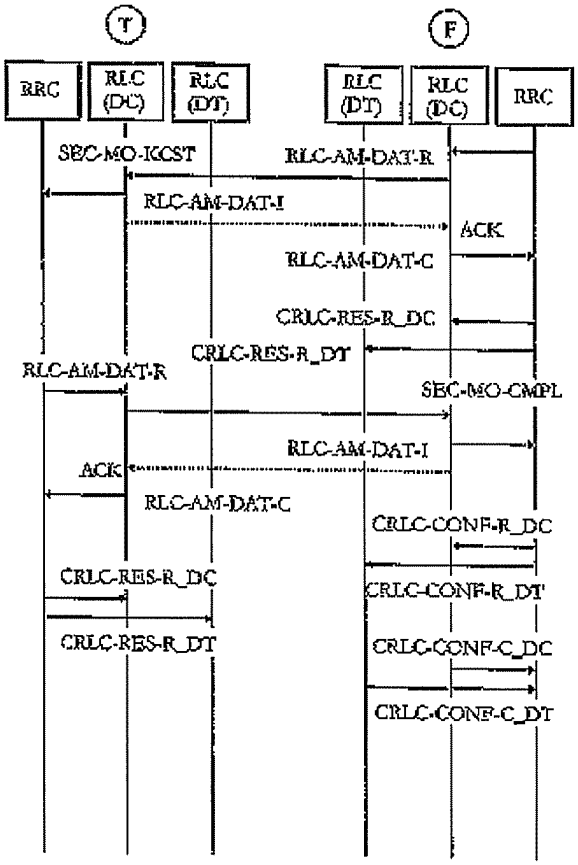
【図９】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
CRLC-S-R(ND_DT)
CRLC-S-R(ND_DC)
CRLC-S-C(VTD_DT)
CRLC-S-C(VTD_DC)
CRLC-CONF-R_DT(CKN)
CRLC-CONF-R_DC(CKN)
CRLC-CONF-C_DT
CRLC-CONF-C_DC
RLC-AM-DAT-R
SEC-MO-CMD
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C

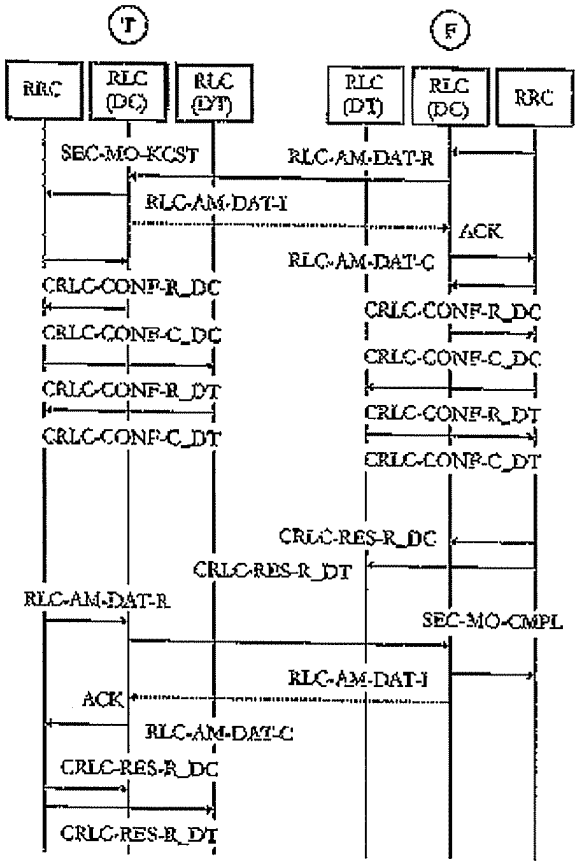
【図１０】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
CRLC-S-R(NU_DC)
CRLC-S-R(NU_DT)
CRLC-S-C(VTU_DC)
CRLC-S-C(VTU_DT)
CRLC-CONF-R_DC(CKN)
CRLC-CONF-R_DT(CKN)
CRLC-CONF-C_DC
CRLC-CONF-C_DT
RLC-AM-DAT-R*
SEC-MO-KC
RLC-AM-DAT-I*
ACK
RLC-AM-DAT-C

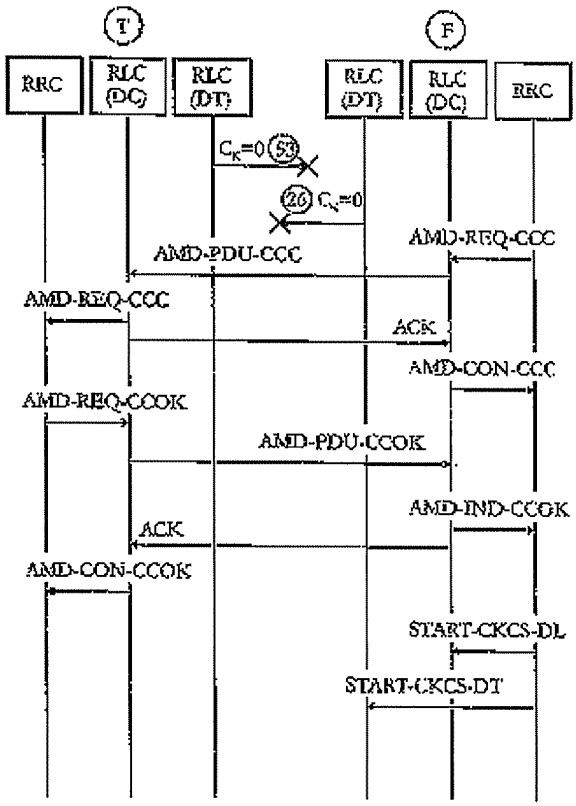
【図１１】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
SEC-MO-KCST
RLC-AM-DAT-R
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C
CRLC-RES-R_DC
CRLC-RES-R_DT
RLC-AM-DAT-R
SEC-MO-CMPL
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C
CRLC-CONF-R_DC
CRLC-RES-R_DC
CRLC-CONF-R_DT
CRLC-RES-R_DT
CRLC-CONF-C_DC
CRLC-CONF-C_DT

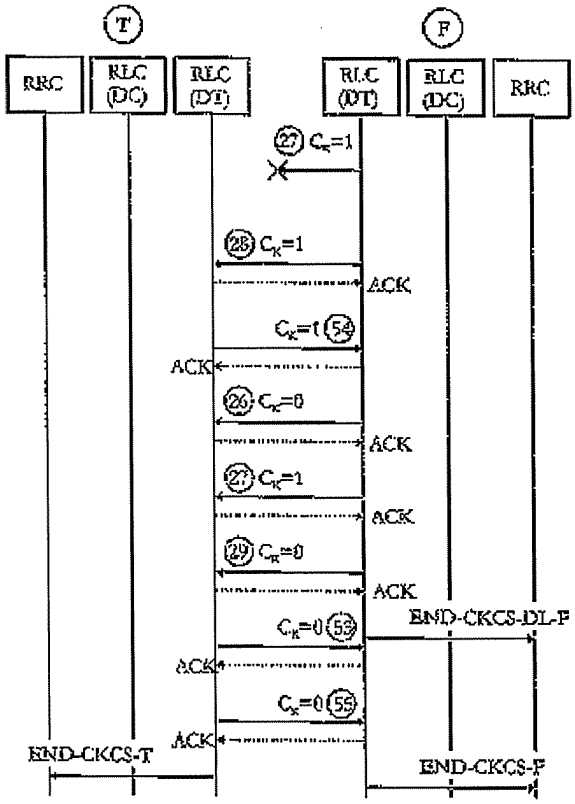
【図１２】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
SEC-MO-KCST
RLC-AM-DAT-R
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C
CRLC-CONF-R_DC
CRLC-CONF-C_DC
CRLC-CONF-R_DT
CRLC-CONF-C_DT
CRLC-RES-R_DC
CRLC-RES-R_DT
RLC-AM-DAT-R
SEC-MO-CMPL
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C
CRLC-RES-R_DC
CRLC-RES-R_DT

【図１３】


T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
C_K=0
53
26
C_K=0
AMD-REQ-CCC
AMD-PDU-CCC
AMD-REQ-CCC
ACK
AMD-CON-CCC
AMD-REQ-CCOK
AMD-PDU-CCOK
AMD-IND-CCOK
ACK
AMD-CON-CCOK
START-CKCS-DL
START-CKCS-DT

【図１４】



フロントページの続き

(31)優先権主張番号　１０００２６３６．２
(32)優先日　平成12年１月21日(2000．１．21)
(33)優先権主張国　ドイツ（ＤＥ）
(31)優先権主張番号　１００１５３８９．５
(32)優先日　平成12年３月28日(2000．３．28)
(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　590000248
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，　Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(72)発明者　ヨーゼフ　ヴァセル
ドイツ連邦共和国，５０１８１　ベドブルク，シュタイフェンザントシュトラーセ　６０